RSAC 2025 Conference

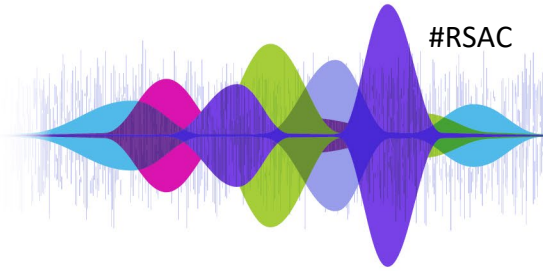
Many Voices.
One Community.

SESSION ID: NCS-W02

Strengthening Network Infrastructure Security in a Complex Threat Landscape

Paul Hopkins
Global Head of Cyber Strategy,
Architecture and Secure by Design

Omar Santos
Distinguished Engineer
Cisco



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- The Evolution of Attacks Against Infrastructure Devices
- Case Studies:
  - Synful Knock
  - Smart Install Protocol Misuse
  - Jaguar Tooth
  - Volt Typhoon
  - Salt Typhoon
- Lessons Learned and Best Practices
- Q&A

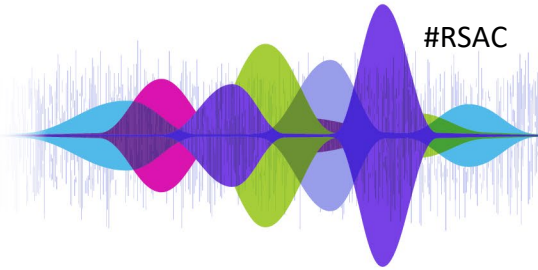
RSAC 2025 Conference

The Evolution of Attacks Against Infrastructure Devices

Insights from Major Cyber Attacks

Many Voices.
One Community.

Insights from Major Cyber Attacks

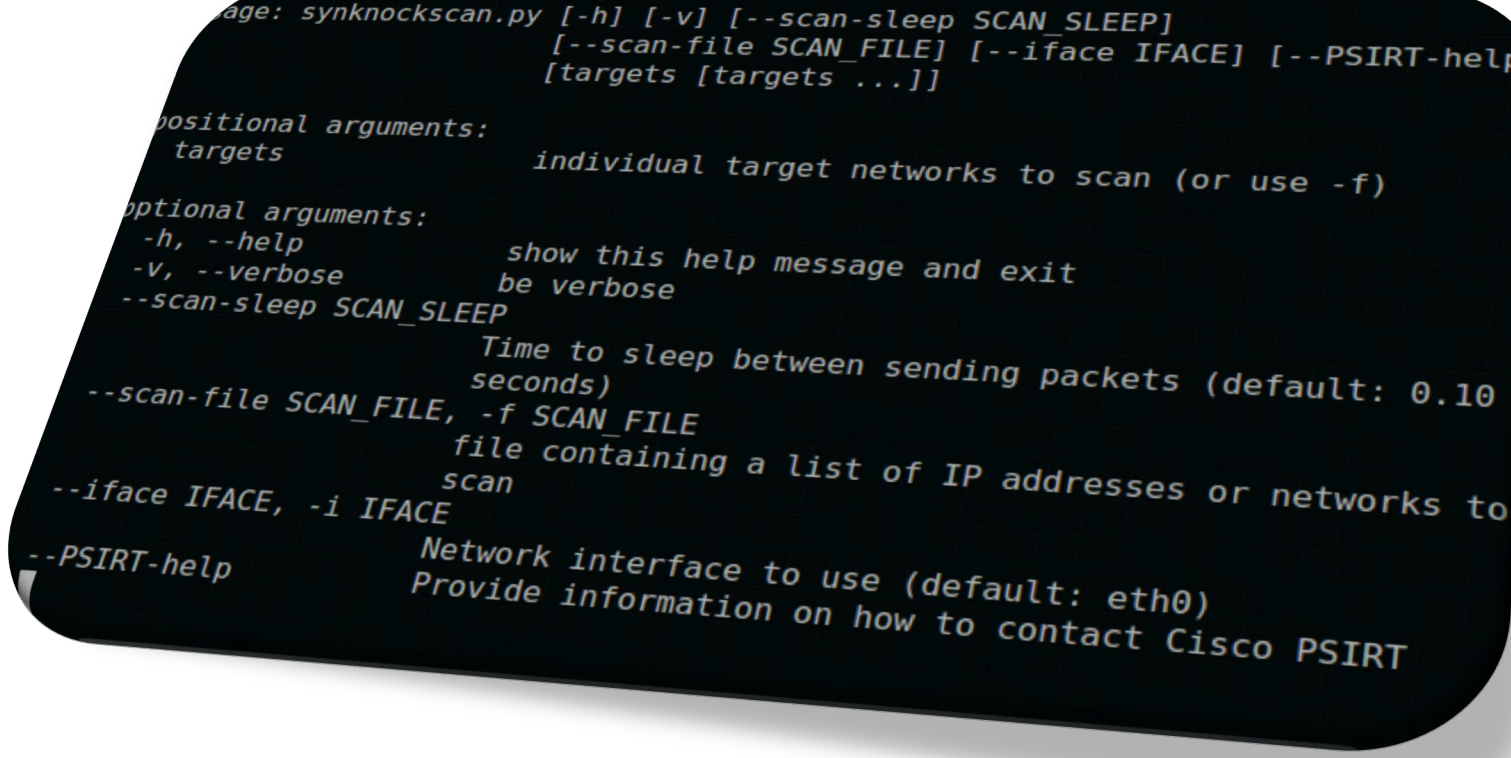


- Attackers continue to focus on exploiting misconfigurations, unpatched vulnerabilities, and weak credentials in network infrastructure in 2025 and beyond.
- High-profile campaigns (e.g., Synful Knock, Jaguar Tooth, Volt Typhoon, Salt Typhoon, and others) highlight the importance of robust security practices that have existed for decades, especially in managing hardware and software lifecycles and protecting credentials.

Synful Knock

First came to light in 2015

Allowed persistent unauthorized access.


age: synknockscan.py [-h] [-v] [--scan-sleep SCAN_SLEEP]
[--scan-file SCAN_FILE] [--iface IFACE] [--PSIRT-help
[targets [targets ...]]
positional arguments:
targets individual target networks to scan (or use -f)
optional arguments:
-h, --help show this help message and exit
-v, --verbose be verbose
--scan-sleep SCAN_SLEEP
Time to sleep between sending packets (default: 0.10
seconds)
--scan-file SCAN_FILE, -f SCAN_FILE
file containing a list of IP addresses or networks to
scan
--iface IFACE, -i IFACE
Network interface to use (default: eth0)
--PSIRT-help Provide information on how to contact Cisco PSIRT

- Attackers leveraged administrative access and firmware weaknesses to install malicious code and remain undetected.
- Modified the translation lookaside buffer (TLB) Read/Write attributes
- Modified a legitimate IOS function to call and initialize the malware
- Overwrote legitimate protocol handling functions with malicious code
- Overwrote strings referenced by legitimate functions with strings used by the malware

https://blogs.cisco.com/security/synful-knock

RSAC 2025 Conference

Smart Install Protocol Misuse

The protocol that was completely broken

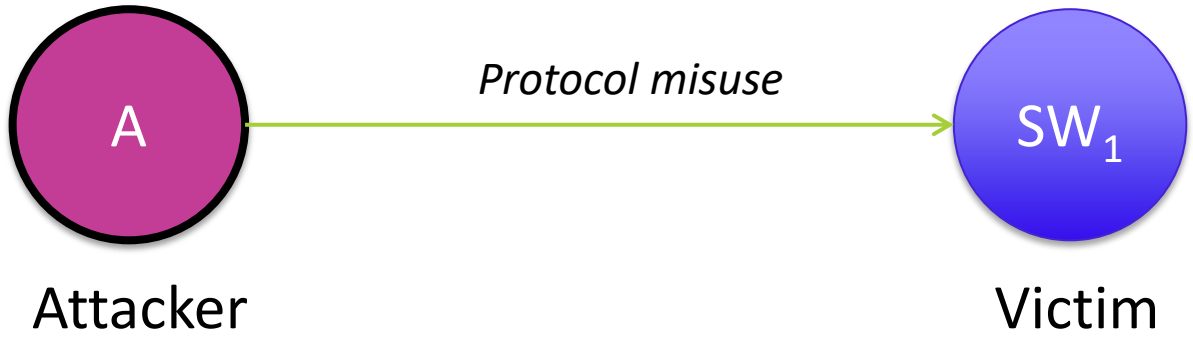
Many Voices.
One Community.

Smart Install

- A protocol that has been deprecated and removed since 2017.
- It was originally designed as a zero-touch deployment feature, allowing new or replacement switches (Smart Install clients) to automatically download their configurations from a Smart Install director without requiring user interaction.

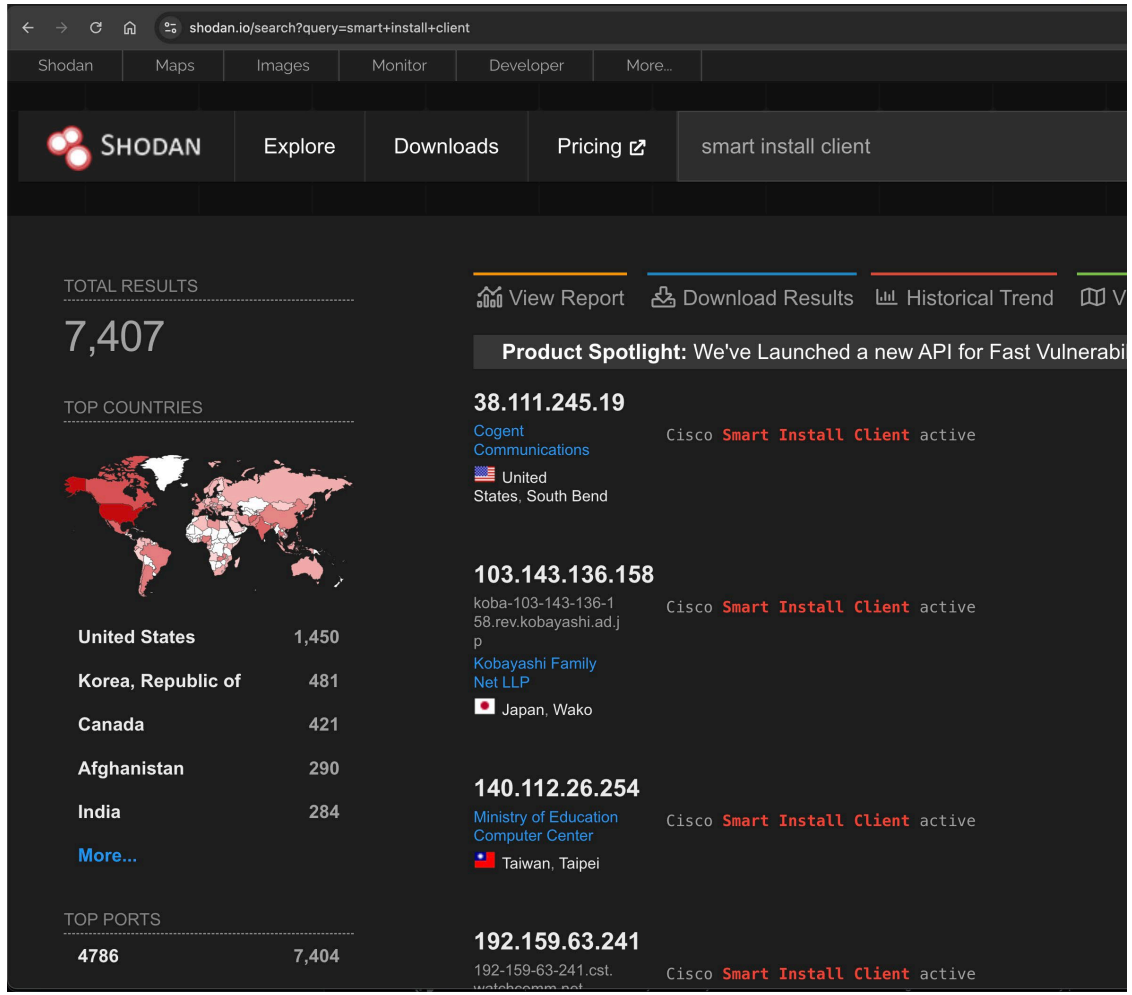
Protocol Misuse

- Malicious actors misused the Smart Install protocol to:
  - Change TFTP server settings on a client switch
  - Copy files from the client switch to an attacker-controlled server
  - Replace the device's startup configuration with malicious files
  - Load an attacker-supplied firmware onto the switch
  - Execute high-privilege CLI commands remotely



It's 2025 and …

- There are still over 7,000 entries in Shodan of potentially exploitable devices.
- Cisco PSIRT, Talos, FBI, CISA, and many other outlets have been warning customers since 2017.



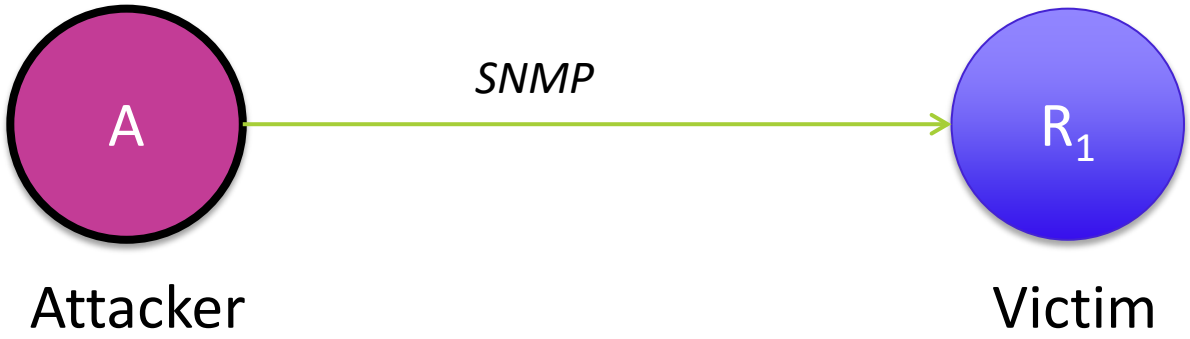
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi

RSAC 2025 Conference

Jaguar Tooth

Jaguar Tooth

- April 18, 2023: the UK National Cyber Security Centre (NCSC), FBI, NSA and CISA published a joint advisory describing how state-sponsored cyber actors were able to successfully exploit a known SNMP vulnerability (CVE-2017-6742).
- This vulnerability was first disclosed in a security advisory on June 29, 2017.



https://blogs.cisco.com/security/threat-actors-exploiting-snmp-vulnerabilities-in-cisco-routers

Malware Analysis Report

Over 19 years old!!!

National Cyber Security Centre
a part of GCHQ

Jaguar Tooth is non-persistent malware that targets Cisco IOS routers running firmware: `C5350-IS-M, Version 12.3(6)`. It includes functionality to collect device information, which it exfiltrates over TFTP, and enables unauthenticated backdoor access. It has been observed being deployed and executed via exploitation of the patched SNMP vulnerability CVE-2017-6742.

https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/jaguar-tooth/NCSC-MAR-Jaguar-Tooth.pdf

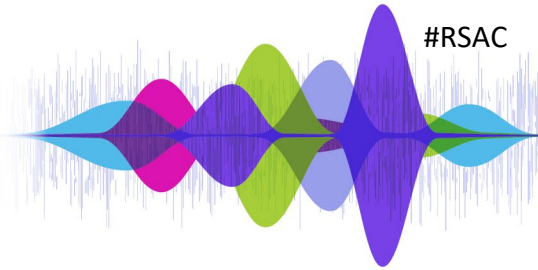
RSAC 2025 Conference

Volt Typhoon

Living-off-the-Land

Many Voices.
One Community.

Volt Typhoon



- Volt Typhoon is a threat group that has been active since at least 2021 and has targeted critical infrastructure.
- Their tactics rely heavily on “living off the land” (using built-in system tools rather than deploying custom malware), making detection far more difficult.
- By focusing attacks on multi-vendor routers, firewalls, and VPN devices, they can hide under normal administrative traffic.

More End-of-life Devices

- The attackers took advantage of pervasive end-of-life and end-of-support devices, several vendors were impacted.
- End-of-life and end-of-support RV-series routers were among the devices that were leveraged by the attackers.
- CISA released comprehensive guidelines aimed at protecting systems from living-off-the-land (LoTL) attacks.

These SMB devices were placed in critical infrastructure and never upgraded (some with default configurations)

Living-off-the-Land Detection Best Practices:

Use UEBA

Integrate UEBA to enhance detection capabilities.

Optimize Alerts

Refine alert systems to reduce noise and focus on critical issues.

Automate Analysis

Implement tools to automate log analysis and detect anomalies.

Activity Baselines

Regularly update baselines for network and user activities.

Robust Logging

Establish detailed and tamper-proof logging systems.

RSAC™ 2025 Conference

Salt Typhoon

Salt Typhoon

- Salt Typhoon is another attack campaign that has exploited misconfigurations in routers, VPNs, and other network hardware provided by different vendors, often leveraging EoL devices that no longer receive updates.
- Cisco is not aware of any new vulnerabilities that are being exploited as part of this attack campaign.
- The attackers exploited poor credential management practices in infrastructure devices.
- This included using stolen credentials, weak or easily guessable passwords, and the lack of multi-factor authentication.

https://blog.talosintelligence.com/salt-typhoon-analysis

Credential Management

- Attackers leveraged valid credentials likely obtained from technology systems not directly managed or controlled by Cisco, to enable access to equipment owned and operated by Cisco customers.
- Attackers used these credentials to gain administrative access.
- Cisco has worked with CISA and other government agencies to continue to provide guidance on how to detect and mitigate such threats.

https://blog.talosintelligence.com/salt-typhoon-analysis

Configuration Exfiltration & Modification

- Attackers exfiltrated sensitive device configurations (via TFTP/FTP), exposing authentication material like SNMP community strings and weakly encrypted local passwords.
- Modifications included changes to AAA/TACACS settings, loopback interface IPs, creation of unauthorized accounts, and unexpected adjustments to access control lists and device services.

https://blog.talosintelligence.com/salt-typhoon-analysis

Tools & Techniques

- The use of living-off-the-land tactics allowed attackers to operate using native network utilities such as Tcpdump, Tpacap, and Embedded Packet Capture.
- A custom tool, “JumbledPath” (written in GO for x86-64 Linux systems), was used to capture packets, clear logs, and obscure the source and destination of malicious activities.

https://blog.talosintelligence.com/salt-typhoon-analysis

Defense Evasion & Persistence

- Routine log clearing (e.g., .bash_history, auth.log) and manipulation of loopback interface addresses were used to bypass access control lists and hide malicious activities.

Mitigation Recommendations:

- Patch known vulnerabilities (e.g., CVE-2018-0171, CVE-2023-20198, CVE-2023-20273, CVE-2024-20399) and disable unnecessary services such as Smart Install and Guest Shell.
- Enhance configuration management, enforce strong access controls, implement good credential management, and secure management protocols with encryption (SSH, HTTPS, SNMPv3).

https://blog.talosintelligence.com/salt-typhoon-analysis

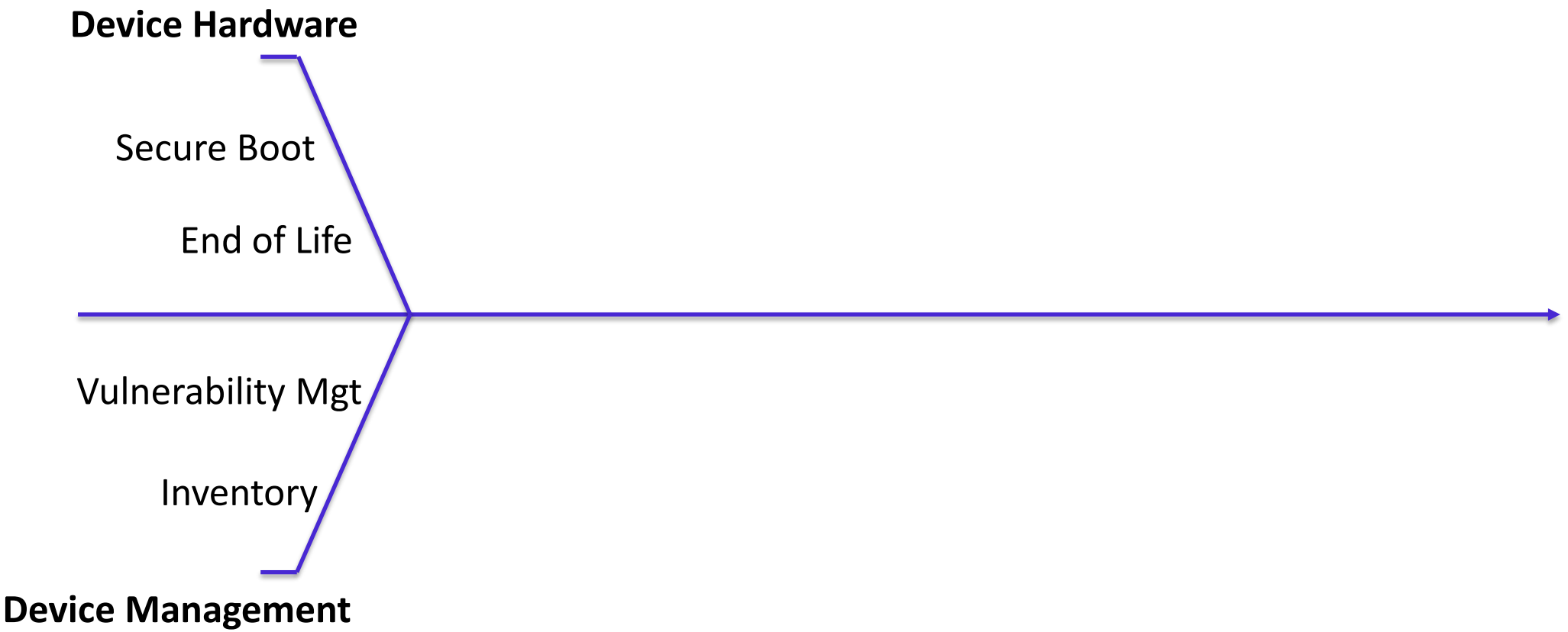
RSAC™ 2025 Conference

Safeguarding your Infrastructure

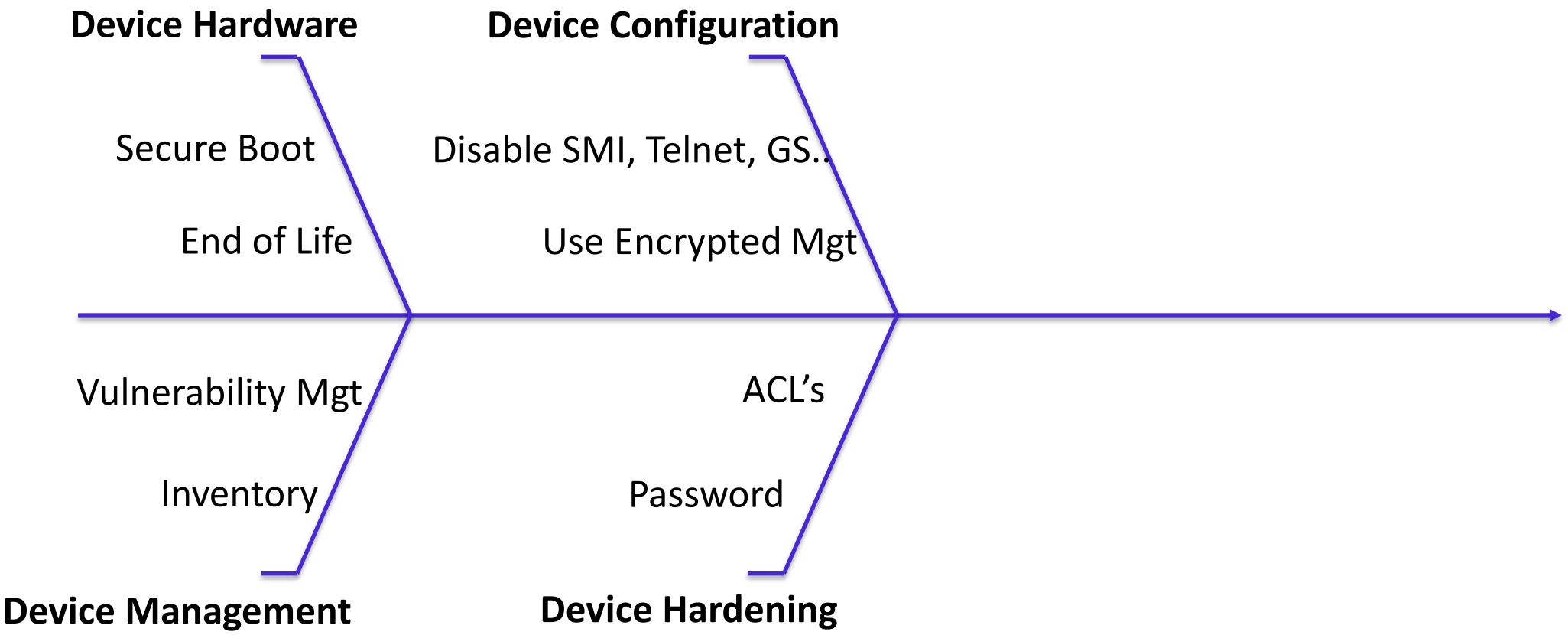
Safeguarding your infrastructure

- Device Measures
  - Secure Boot
  - Vulnerability Management
  - Hardening
- System Measures
  - Access Control
  - Credential Management
  - Logging & Monitoring
  - Management Plane Design

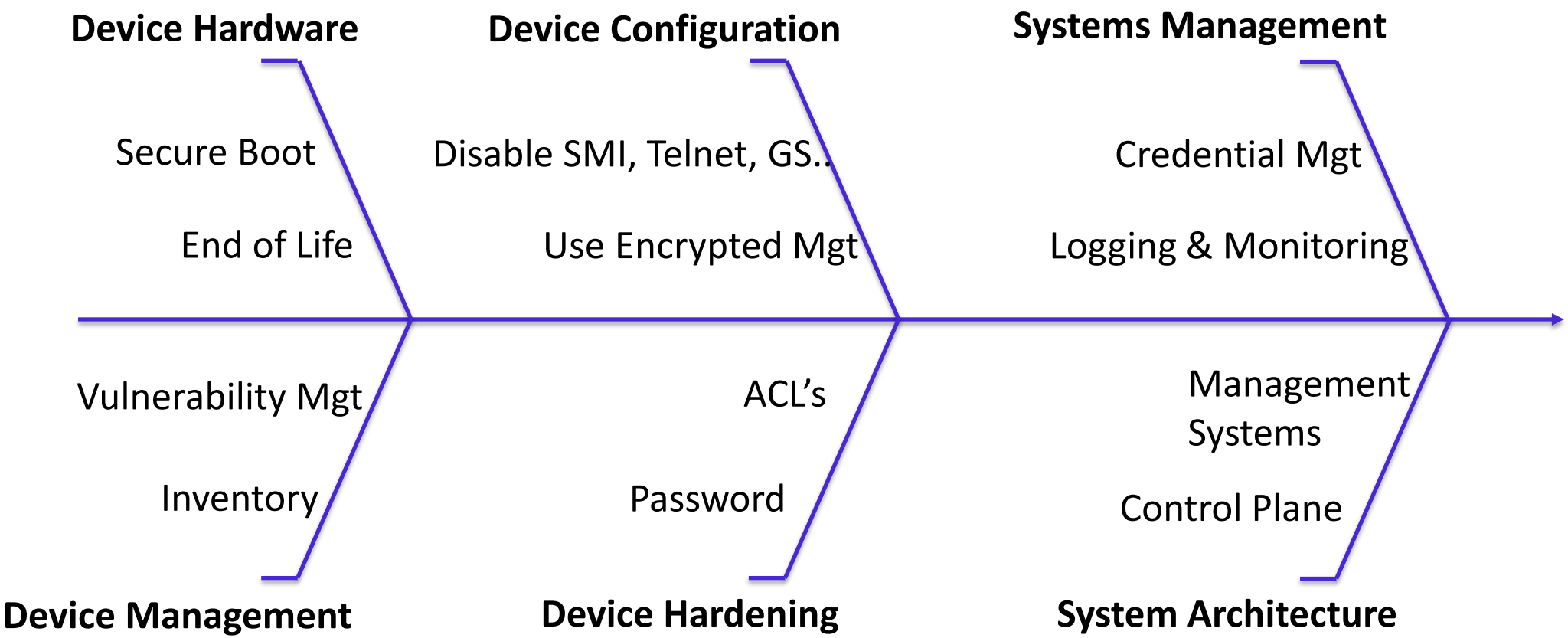
Reducing Risk of Exploitation



Reducing Risk of Exploitation



Reducing Risk of Exploitation



Apply

- Next week you should
  - Identify Perimeter Devices & vulnerability status.
- In next 3 months you should
  - Continuous vulnerability management programme
  - Continuous hardening and checking of individual devices
  - Enhance Logging & Monitoring
- In next 12 months you should
  - Review credential & access control lists.
  - Review management architecture.
  - Secure Boot/Firmware measures.
  - Plan for End of Life

RSAC™ 2025 Conference

Many Voices.
One Community.